The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/11/2016

SUBJECT:
Cumulative Security Update for Microsoft Edge (MS16-119)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Edge, the most severe of which could allow remote code execution if a user views a specially crafted web page. Microsoft Edge replaced Internet Explorer as the default browser on Windows 10. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are reports of a scripting engine remote code execution vulnerability (CVE-2016-7189) being exploited in the wild.

SYSTEMS AFFECTED:

- Windows 10
- Windows 10 (Version 1511)
- Windows 10 (Version 1607)

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Edge that could allow for remote code execution. Details of these vulnerabilities are as follows:

- One memory corruption vulnerability exists when Microsoft Edge improperly handles objects in memory (CVE-2016-3331)
- Six scripting engine memory corruption vulnerabilities exist in the way the Chakra JavaScript engine renders when handling objects in memory (CVE-2016-3382, CVE-2016-3386, CVE-2016-3389, CVE-2016-3390, CVE-2016-7190, CVE-2016-7194)
- One information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory (CVE-2016-3267)
- One information disclosure vulnerability exists when Microsoft Edge leaves credential data in memory (CVE-2016-3391)
- One scripting engine remote code execution vulnerability exists when Microsoft Edge improperly handles objects in memory (CVE-2016-7189)
- Two elevation of privilege vulnerabilities exist when Microsoft Edge fails to properly secure private namespace (CVE-2016-3388, CVE-2016-3387)
- One security bypass vulnerability exists when the Edge Content Security Policy Fails to properly handle validation of certain specially crafted documents (CVE-2016-3392)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:
https://technet.microsoft.com/en-us/library/security/ms16-119.aspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3267
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3331
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3382
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3386
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3387
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3388

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3389
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3390
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3391
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3392
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7189
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7190
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7194